II

(Ne teisėkūros procedūra priimami aktai)

SPRENDIMAI

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2020/1023

2020 m. liepos 15 d.

kuriuo dėl nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinio keitimosi duomenimis kovojant su COVID-19 pandemija iš dalies keičiamas Įgyvendinimo sprendimas (ES) 2019/1765

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyvą 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo ([1]), ypač į jos 14 straipsnio 3 dalį,

kadangi:

(1) pagal Direktyvos 2011/24/ES 14 straipsnį Sąjunga remia valstybių narių bendradarbiavimą ir keitimąsi informacija savanoriškame tinkle, vienijančiame valstybių narių paskirtas už e. sveikatą atsakingas nacionalines institucijas (toliau – e. sveikatos tinklas), ir tam sudaro palankias sąlygas;

(2) Komisijos įgyvendinimo sprendimu (ES) 2019/1765 ([2]) nustatomos už e. sveikatą atsakingų nacionalinių institucijų tinklo sukūrimo, valdymo ir veikimo taisyklės. To sprendimo 4 straipsniu e. sveikatos tinklui pavesta padėti gerinti nacionalinių informacinių ir ryšių technologijų sistemų sąveiką ir elektroninių sveikatos duomenų tarpvalstybinį perdavimą teikiant tarpvalstybines sveikatos priežiūros paslaugas;

(3) atsižvelgdamos į visuomenės sveikatos krizę, kurią sukėlė COVID-19 pandemija, kelios valstybės narės sukūrė programėles, kurios padeda atsekti kontaktus ir suteikia galimybę įspėti tokių programėlių naudotojus imtis atitinkamų veiksmų, tokių kaip tyrimas arba saviizoliacija, jei jie galėjo užsikrėsti virusu būdami arti kito tokių programėlių naudotojo, kuris pranešė apie teigiamą diagnozę. Šios programėlės artumui tarp įrenginių nustatyti naudoja „Bluetooth“ technologiją. Nuo 2020 m. birželio mėn. ėmus naikinti kelionių iš vienos valstybės narės į kitą apribojimus, e. sveikatos tinklui priklausančios valstybės narės turėtų užtikrinti didesnę nacionalinių informacinių ir ryšių technologijų sistemų sąveiką diegdamos skaitmeninę infrastruktūrą, sudarančią sąlygas nacionalinių programėlių, padedančių atsekti kontaktus ir įspėti naudotojus, sąveikai;

([1]) OL L 88, 2011 4 4, p. 45.

([2]) 2019 m. spalio 22 d. Komisijos įgyvendinimo sprendimas (ES) 2019/1765, kuriuo nustatomos už e. sveikatą atsakingų nacionalinių institucijų tinklo sukūrimo, valdymo ir veikimo taisyklės ir panaikinamas Įgyvendinimo sprendimas 2011/890/ES (OL L 270, 2019 10 24, p. 83).

(4) Komisija valstybėms narėms teikia su pirmiau nurodytomis programėlėmis susijusią paramą. 2020 m. balandžio 8 d. Komisija priėmė Rekomendaciją dėl bendro Sąjungos priemonių rinkinio technologijoms ir duomenims, visų pirma mobiliosioms programėlėms ir anonimintiems judumo duomenims, naudoti kovojant su COVID-19 krize ir siekiant ją įveikti (toliau – Komisijos rekomendacija) ([3]). E. sveikatos tinklui priklausančios valstybės narės, padedamos Komisijos, priėmė bendrą ES priemonių rinkinį valstybėms narėms, skirtą atsekti kontaktus padedančioms programėlėms ([4]), ir Patvirtintų kontaktų atsekimo programėlių ES sąveikos gaires ([5]). Priemonių rinkinyje paaiškinami nacionaliniai reikalavimai, taikomi nacionalinėms kontaktų atsekimo ir įspėjimo programėlėms, visų pirma tai, kad jos turėtų būti savanoriškos, jas turėtų būti patvirtinusi atitinkama nacionalinė sveikatos institucija, jomis turėtų būti užtikrinamas privatumas ir jos turėtų būti pašalintos, kai tik jų nebereikia. Atsižvelgdamos į naujausius su COVID-19 krize susijusius pokyčius, Komisija ([6]) ir Europos duomenų apsaugos valdyba ([7]) paskelbė su duomenų apsauga susijusias programėlių ir kontaktų atsekimo priemonių gaires. Valstybių narių programėlės ir skaitmeninė infrastruktūra, sudaranti sąlygas jų sąveikai, projektuojamos remiantis bendru ES priemonių rinkiniu, pirmiau nurodytomis gairėmis ir techninėmis specifikacijomis, dėl kurių sutarta e. sveikatos tinkle;

(5) siekdamos palengvinti nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką, e. sveikatos tinkle dalyvaujančios valstybės narės, kurios nusprendė savanoriškai aktyviau bendradarbiauti šioje srityje, padedamos Komisijos sukūrė skaitmeninę infrastruktūrą kaip IT priemonę keitimuisi duomenimis. Ši skaitmeninė infrastruktūra vadinama sietiniu tinklų sietuvu;

(6) šiame sprendime nustatomos nuostatos dėl dalyvaujančių valstybių narių ir Komisijos vaidmens užtikrinant nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinei sąveikai skirto sietinio tinklų sietuvo veikimą;

(7) kontaktų atsekimo ir įspėjimo programėlių naudotojų asmens duomenų tvarkymas, už kurį atsako valstybės narės arba kitos viešosios organizacijos ar oficialios įstaigos valstybėse narėse, turėtų būti atliekamas laikantis Europos Parlamento ir Tarybos reglamento (ES) 2016/679 ([8]) (Bendrojo duomenų apsaugos reglamento) ir Europos Parlamento ir Tarybos direktyvos 2002/58/EB ([9]). Asmens duomenų tvarkymas, už kurį atsako Komisija, sietinio tinklų sietuvo valdymo ir saugumo užtikrinimo tikslu turėtų atitikti Europos Parlamento ir Tarybos reglamentą (ES) 2018/1725 ([10]);

(8) sietinį tinklų sietuvą turėtų sudaryti saugi bendrą sąsają teikianti IT infrastruktūra, kuria naudodamosi paskirtosios nacionalinės institucijos arba oficialios įstaigos galėtų keistis minimaliu duomenų rinkiniu, susijusiu su kontaktu su SARS-CoV-2 užsikrėtusiais asmenimis, kad būtų galima informuoti kitus asmenis apie galimą jų užsikrėtimą ta infekcija, ir kuri skatina valstybes nares veiksmingai bendradarbiauti sveikatos priežiūros klausimais, nes naudojant šią infrastruktūrą keistis svarbia informacija būtų lengviau;

(9) todėl šiame sprendime turėtų būti nustatytos paskirtųjų nacionalinių institucijų arba oficialių įstaigų tarpvalstybinio keitimosi duomenimis naudojantis sietiniu tinklų sietuvu ES sąlygos;

([3]) 2020 m. balandžio 8 d. Komisijos rekomendacija (ES) 2020/518 dėl bendro Sąjungos priemonių rinkinio technologijoms ir duomenims, visų pirma mobiliosioms programėlėms ir anonimintiems judumo duomenims, naudoti kovojant su COVID-19 krize ir siekiant ją įveikti (OL L 114, 2020 4 14, p. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Komisijos komunikatas „Duomenų apsaugos gairės dėl kovai su COVID-19 pandemija naudojamų programėlių“ (OL C 124I, 2020 4 17, p. 1).

([7]) Gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių naudojimo COVID-19 protrūkio aplinkybėmis ir 2020 m. birželio 16 d. EDAV pareiškimas dėl kontaktų atsekimo programėlių sąveikumo poveikio duomenų apsaugai. Abu dokumentai skelbiami adresu https://edpb.europa.eu.

([8]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

([9]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

([10]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

(10) dalyvaujančios valstybės narės, kurioms atstovauja paskirtosios nacionalinės institucijos arba oficialios įstaigos, kartu nustato asmens duomenų tvarkymo naudojant sietinį tinklų sietuvą tikslą ir priemones, todėl jos laikomos bendromis duomenų valdytojomis. Bendrojo duomenų apsaugos reglamento 26 straipsniu asmens duomenų tvarkymo operacijų bendri duomenų valdytojai įpareigojami skaidriai nustatyti atitinkamą savo atsakomybę už pagal tą reglamentą nustatytų įpareigojimų vykdymą. Jame taip pat numatyta galimybė, kad minėta atsakomybė būtų nustatyta Sąjungos arba valstybės narės teisėje, kuri yra taikoma duomenų valdytojams. Kiekvienas duomenų valdytojas turėtų užtikrinti, kad jis turėtų nacionalinio lygmens teisinį pagrindą duomenų tvarkymui sietiniame tinklų sietuve;

(11) Komisija yra techninių ir organizacinių su sietiniu tinklų sietuvu susijusių sprendimų teikėja, todėl ji dalyvaujančių valstybių narių (bendrų duomenų valdytojų) vardu tvarko pseudoniminius asmens duomenis sietiniame tinklų sietuve ir yra laikoma duomenų tvarkytoja. Pagal Bendrojo duomenų apsaugos reglamento 28 straipsnį ir Reglamento (ES) 2018/1725 29 straipsnį duomenų tvarkytojo atliekamas duomenų tvarkymas reglamentuojamas sutartimi arba teisės aktu pagal Sąjungos arba valstybės narės teisę, kurie yra privalomi duomenų tvarkytojui duomenų valdytojo atžvilgiu ir kuriuose nustatomas konkretus duomenų tvarkymas. Šiuo sprendimu nustatomos Komisijos kaip duomenų tvarkytojos atliekamo duomenų tvarkymo taisyklės;

(12) kai Komisija tvarko asmens duomenis sietiniame tinklų sietuve, ji privalo laikytis Komisijos sprendimo (ES, Euratomas) 2017/46 ([11]);

(13) atsižvelgiant į tai, kad siekiant tikslų, kuriais duomenų valdytojai tvarko asmens duomenis nacionalinėse kontaktų atsekimo ir įspėjimo programėlėse, nebūtinai reikia nustatyti duomenų subjekto tapatybę, duomenų valdytojai ne visada gali būti pajėgūs užtikrinti duomenų subjektų teisių taikymą. Todėl Bendrojo duomenų apsaugos reglamento 15–20 straipsniuose nurodytos teisės gali būti netaikomos, kai įvykdomos to reglamento 11 straipsnyje nustatytos sąlygos;

(14) reikia pakeisti galiojančio Įgyvendinimo sprendimo (ES) 2019/1765 priedo numeraciją, nes pridedami du nauji priedai;

(15) todėl Įgyvendinimo sprendimas (ES) 2019/1765 turėtų būti atitinkamai iš dalies pakeistas;

(16) atsižvelgiant į tai, kad būtina skubiai reaguoti į padėtį, susidariusią dėl COVID-19 pandemijos, šis sprendimas turėtų būti taikomas nuo kitos dienos po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*;

(17) vadovaujantis Reglamento (ES) 2018/1725 42 straipsnio 1 dalimi buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis 2020 m. liepos 9 d. pateikė nuomonę;

(18) šiame sprendime numatytos priemonės atitinka Direktyvos 2011/24/ES 16 straipsniu įsteigto Komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Įgyvendinimo sprendimas 2019/1765 iš dalies keičiamas taip:

1. 2 straipsnio 1 dalyje įterpiami šie g, h, i, j, k, l, m, n ir o punktai:

„g) programėlės naudotojas – išmanųjį įrenginį turintis asmuo, kuris parsisiuntė ir naudoja patvirtintą kontaktų atsekimo ir įspėjimo programėlę;

h) kontaktų atsekimas – priemonės, kurios įgyvendinamos siekiant atsekti asmenis, kurie turėjo sąlytį su didelės tarpvalstybinio pobūdžio grėsmės sveikatai šaltiniu, kaip tai suprantama Europos Parlamento ir Tarybos sprendimo Nr. 1082/2013/ES (*) 3 straipsnio c punkte;

([11]) 2017 m. sausio 10 d. Komisijos sprendimo (ES, Euratomas) 2017/46 dėl Europos Komisijos ryšių ir informacinių sistemų saugumo (OL L 6, 2017 1 11, p. 40). Daugiau informacijos apie visoms Europos Komisijos informacinėms sistemoms taikomus saugumo standartus Komisija skelbia adresu https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.

i) nacionalinė kontaktų atsekimo ir įspėjimo programėlė – nacionaliniu lygmeniu patvirtinta ir išmaniuosiuose įrenginiuose, visų pirma išmaniuosiuose telefonuose, veikianti programinė įranga, kuri paprastai yra suprojektuota įvairiai ir tikslingai sąveikai su interneto ištekliais užtikrinti ir kuri apdoroja daugelio išmaniuosiuose įrenginiuose esančių jutiklių surinktus artumo duomenis ir kitą kontekstinę informaciją kontakto su SARS-CoV-2 užsikrėtusiais asmenimis atsekimo ir asmenų, kurie galėjo užsikrėsti SARS-CoV-2, įspėjimo tikslais. Šios programėlės gali nustatyti kitus arti esančius ir „Bluetooth“ naudojančius įrenginius ir keistis informacija su vidiniais serveriais (angl. „backend servers“) naudodamosi internetu;

j) sietinis tinklų sietuvas – naudojantis saugia IT priemone Komisijos valdomas nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką užtikrinantis tinklų sietuvas, į kurį iš valstybių narių vidinių serverių gaunamas, kuriame saugomas ir iš kurio joms teikiamas minimalus asmens duomenų rinkinys;

k) raktas – programėlės naudotojo, pranešančio, kad užsikrėtė ar galėjo užsikrėsti SARS-CoV-2, unikalus trumpalaikis identifikatorius;

l) informacijos apie infekciją patvirtinimas – metodas, taikomas informacijai apie SARS-CoV-2 infekciją patvirtinti, t. y. ar apie ją pranešė pats programėlės naudotojas, ar ją patvirtino nacionalinė sveikatos priežiūros institucija, ar ji buvo patvirtinta laboratoriniu tyrimu;

m) susijusios šalys – valstybė narė arba valstybės narės, kurioje (-iose) programėlės naudotojas buvo per 14 dienų iki raktų įkėlimo dienos ir kurioje (-iose) jis parsisiuntė patvirtintą nacionalinę kontaktų atsekimo ir įspėjimo programėlę ir (arba) keliavo;

n) raktų kilmės šalis – valstybė narė, kurioje yra vidinis serveris, iš kurio įkelti raktai į sietinį tinklų sietuvą;

o) žurnalo duomenys – automatinis įrašas apie veiklą, susijusią su keitimusi duomenimis, tvarkomais per sietinį tinklų sietuvą, ir prieiga prie jų, iš kurio visų pirma matyti tvarkymo veiklos rūšis, tvarkymo veiklos data ir laikas ir duomenis tvarkančio asmens identifikatorius.

_____

(*) 2013 m. spalio 22 d. Europos Parlamento ir Tarybos sprendimas Nr. 1082/2013/ES dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 2119/98/EB (OL L 293, 2013 11 5, p. 1).“

2. 4 straipsnio 1 dalyje įterpiamas šis h punktas:

„h) teikti valstybėms narėms gaires dėl nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinio keitimosi asmens duomenimis per sietinį tinklų sietuvą.“

3. 6 straipsnio 1 dalyje įterpiami šie f ir g punktai:

„f) rengia, įgyvendina ir prižiūri atitinkamas technines ir organizacines priemones, susijusias su asmens duomenų perdavimo ir prieglobos sietiniame tinklų sietuve saugumu, nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveikos užtikrinimo tikslu;

g) remia e. sveikatos tinklą pritardama techninei ir organizacinei nacionalinių institucijų atitikčiai tarpvalstybinio keitimosi asmens duomenimis sietiniame tinklų sietuve reikalavimams, numatydama ir atlikdama tam būtinus bandymus ir auditus. Komisijos auditoriams gali padėti valstybių narių ekspertai.“

4. 7 straipsnis iš dalies keičiamas taip:

a) pavadinimas pakeičiamas taip: „Per e. sveikatos skaitmeninių paslaugų infrastruktūrą tvarkomų asmens duomenų apsauga“;

b) 2 dalyje žodis „priede“ pakeičiamas žodžiu „I priede“.

5. Įterpiamas šis 7a straipsnis:

„*7a straipsnis*

Nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinis keitimasis duomenimis per sietinį tinklų sietuvą

1. Kai per sietinį tinklų sietuvą keičiamasi asmens duomenimis, duomenys tvarkomi tik tam, kad būtų galima palengvinti nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką sietiniame tinklų sietuve ir kontaktų atsekimo tęstinumą tarpvalstybinėmis aplinkybėmis.

2. 3 dalyje nurodyti asmens duomenys sietiniam tinklų sietuvui perduodami pseudoniminiu formatu.

3. Pseudoniminiai asmens duomenys, kuriais keičiamasi per sietinį tinklų sietuvą ir kurie jame tvarkomi, apima tik šią informaciją:

a) raktus, kuriuos perduoda nacionalinės kontaktų atsekimo ir įspėjimo programėlės per ne daugiau kaip 14 dienų iki raktų įkėlimo dienos;

b) su raktais susijusius žurnalo duomenis, laikantis techninių specifikacijų protokolo, naudojamo raktų kilmės šalyje;

c) informacijos apie infekciją patvirtinimą;

d) susijusias šalis ir raktų kilmės šalį.

4. Paskirtosios nacionalinės institucijos arba oficialios įstaigos, tvarkančios asmens duomenis sietiniame tinklų sietuve, yra bendros sietiniame tinklų sietuve tvarkomų duomenų valdytojos. Atitinkama bendrų duomenų valdytojų atsakomybė paskirstoma taip, kaip nustatyta II priede. Kiekviena nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinio keitimosi duomenimis sistemoje dalyvauti norinti valstybė narė prieš prisijungdama praneša Komisijai apie savo ketinimą ir nurodo nacionalinę instituciją arba oficialią įstaigą, kuri buvo paskirta atsakinga duomenų valdytoja.

5. Komisija yra sietiniame tinklų sietuve tvarkomų asmens duomenų tvarkytoja. Kaip duomenų tvarkytoja Komisija užtikrina asmens duomenų tvarkymo, įskaitant perdavimą ir prieglobą, sietiniame tinklų sietuve saugumą ir laikosi III priede nustatytų duomenų tvarkytojos įpareigojimų.

6. Komisija ir nacionalinės institucijos, turinčios prieigos prie sietinio tinklų sietuvo teisę, reguliariai bando, tikrina ir vertina techninių ir organizacinių priemonių, kuriomis užtikrinamas asmens duomenų tvarkymo sietiniame tinklų sietuve saugumas, veiksmingumą.

7. Nedarant poveikio bendrų duomenų valdytojų sprendimui nutraukti duomenų tvarkymą sietiniame duomenų sietuve, sietinio duomenų sietuvo veikimas deaktyvinamas ne vėliau kaip 14 dienų po to, kai visos susietos nacionalinės kontaktų atsekimo ir įspėjimo programėlės nustoja perdavinėti raktus per sietinį tinklų sietuvą.“

6. Priedas tampa I priedu.

7. Pridedami II ir III priedai, kurių tekstas pateikiamas šio sprendimo priede.

2 straipsnis

Šis sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Briuselyje 2020 m. liepos 15 d.

Komisijos vardu

Pirmininkė

Ursula VON DER LEYEN

PRIEDAS

Įgyvendinimo sprendimas (ES) 2019/1765 papildomas šiais II ir III priedais:

„II PRIEDAS

DALYVAUJANČIŲ VALSTYBIŲ NARIŲ KAIP SIETINIO TINKLŲ SIETUVO BENDRŲ DUOMENŲ VALDYTOJŲ ATSAKOMYBĖ UŽ TARPVALSTYBINĮ NACIONALINIŲ KONTAKTŲ ATSEKIMO IR ĮSPĖJIMO PROGRAMĖLIŲ VIENŲ KITOMS PERDUODAMŲ DUOMENŲ TVARKYMĄ

1 SKIRSNIS

1 poskirsnis

Atsakomybės pasidalijimas

1) Bendri duomenų valdytojai per sietinį tinklų sietuvą perduodamus asmens duomenis tvarko vadovaudamiesi e. sveikatos tinklo nustatytomis techninėmis specifikacijomis ([1]).

2) Kiekvienas duomenų valdytojas atsako už asmens duomenų tvarkymą sietiniame tinklų sietuve pagal Bendrąjį duomenų apsaugos reglamentą ir Direktyvą 2002/58/EB.

(3) Kiekvienas duomenų valdytojas įsteigia kontaktinį centrą, turintį funkcinę e. pašto dėžutę ryšiams tarp bendrų duomenų valdytojų ir tarp bendrų duomenų valdytojų ir duomenų tvarkytojo palaikyti.

4) Pagal 5 straipsnio 4 dalį e. sveikatos tinklo įsteigtam laikinam pogrupiui pavedama nagrinėti visus klausimus, kylančius dėl nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveikos ir dėl susijusio asmens duomenų tvarkymo bendro valdymo, ir palengvinti suderintų nurodymų Komisijai kaip duomenų tvarkytojai teikimą. Be kitų klausimų, duomenų valdytojai laikiname pogrupyje gali imtis veiksmų, kad suformuluotų bendrą požiūrį į duomenų saugojimą jų nacionaliniuose vidiniuose serveriuose, atsižvelgdami į sietiniame tinklų sietuve nustatytą saugojimo laikotarpį.

5) Nurodymus duomenų tvarkytojui siunčia bet kuris iš bendrų duomenų valdytojų kontaktinių centrų, susitaręs su kitais bendrais duomenų valdytojais pirmiau nurodytame pogrupyje.

6) Tik paskirtųjų nacionalinių institucijų arba oficialių įstaigų įgalioti asmenys gali susipažinti su naudotojų asmens duomenimis, kuriais keičiamasi sietiniame tinklų sietuve.

7) Kiekviena paskirtoji nacionalinė institucija arba oficiali įstaiga nustoja būti bendra duomenų valdytoja nuo jos pasitraukimo iš sietinio tinklų sietuvo dalyvių dienos. Tačiau ji toliau yra atsakinga už duomenų sietiniame tinklų sietuve tvarkymą, atliktą iki jos pasitraukimo.

2 poskirsnis

Su duomenų subjektų prašymų nagrinėjimu ir duomenų subjektų informavimu susijusi atsakomybė ir funkcijos

1) Kiekvienas duomenų valdytojas savo nacionalinės kontaktų atsekimo ir įspėjimo programėlės naudotojams (toliau – duomenų subjektai) pagal Bendrojo duomenų apsaugos reglamento 13 ir 14 straipsnius pateikia informaciją apie jų asmens duomenų tvarkymą sietiniame tinklų sietuve nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinės sąveikos tikslais.

2) Kiekvienas duomenų valdytojas veikia kaip kontaktinis centras savo nacionalinės kontaktų atsekimo ir įspėjimo programėlės naudotojams ir nagrinėja prašymus, susijusius su naudojimusi duomenų subjektų teisėmis pagal Bendrąjį duomenų apsaugos reglamentą, kuriuos pateikia tie naudotojai arba jų atstovai. Kiekvienas duomenų valdytojas paskiria specialų kontaktinį centrą, skirtą iš duomenų subjektų gaunamiems prašymams nagrinėti. Jei bendras duomenų valdytojas iš duomenų subjekto gauna prašymą, kuris nepatenka į jo atsakomybės sritį, jis nedelsdamas persiunčia jį atsakingam bendram duomenų valdytojui. Jei paprašoma, bendri duomenų valdytojai padeda vieni kitiems nagrinėti duomenų subjektų prašymus ir atsako vieni kitiems nepagrįstai nedelsdami ir ne vėliau kaip per 15 dienų nuo pagalbos prašymo gavimo.

([1]) Visų pirma 2020 m. birželio 16 d. Tarpvalstybinių perdavimo grandinių tarp patvirtintų programėlių sąveikos specifikacijomis, skelbiamomis adresu https://ec.europa.eu/health/ehealth/key_documents_lt#anchor0.

3) Kiekvienas duomenų valdytojas duomenų subjektams pateikia šio priedo turinį, be kita ko, nurodydamas 1 ir 2 punktuose nustatytą tvarką.

2 SKIRSNIS

Saugumo incidentų, įskaitant asmens duomenų saugumo pažeidimus, valdymas

1) Bendri duomenų valdytojai padeda vieni kitiems nustatyti ir nagrinėti bet kokius saugumo incidentus, įskaitant asmens duomenų saugumo pažeidimus, susijusius su duomenų tvarkymu sietiniame tinklų sietuve.

2) Visų pirma bendri duomenų valdytojai vieni kitiems praneša apie:

a) bet kokią galimą arba faktinę riziką sietiniame tinklų sietuve tvarkomų asmens duomenų prieinamumui, konfidencialumui ir (arba) vientisumui;

b) bet kokius saugumo incidentus, susijusius su duomenų tvarkymo operacija sietiniame tinklų sietuve;

c) bet kokį asmens duomenų saugumo pažeidimą, galimus asmens duomenų saugumo pažeidimo padarinius ir rizikos fizinių asmenų teisėms ir laisvėms vertinimą, ir bet kokias priemones, kurių imtasi asmens duomenų saugumo pažeidimui pašalinti ir rizikai fizinių asmenų teisėms ir laisvėms sumažinti;

d) bet kokį su duomenų tvarkymo sietiniame tinklų sietuve operacija susijusių techninių ir (arba) organizacinių apsaugos priemonių pažeidimą.

3) Apie bet kokius asmens duomenų saugumo pažeidimus, susijusius su duomenų tvarkymo sietiniame tinklų sietuve operacija, bendri duomenų valdytojai pagal Reglamento (ES) 2016/679 33 ir 34 straipsnius arba gavę Komisijos pranešimą praneša Komisijai, kompetentingoms priežiūros institucijoms ir, kai būtina, duomenų subjektams.

3 SKIRSNIS

Poveikio duomenų apsaugai vertinimas

Jei tam, kad duomenų valdytojas galėtų laikytis Bendrojo duomenų apsaugos reglamento 35 ir 36 straipsniuose nurodytų įpareigojimų, jam reikia informacijos iš kito duomenų valdytojo, jis siunčia specialų prašymą į 1 skirsnio 1 poskirsnio 3 punkte nurodytą funkcinę e. pašto dėžutę. Duomenų valdytojas, kuriam skirtas prašymas, deda visas pastangas, kad pateiktų tokią informaciją.

III PRIEDAS

KOMISIJOS KAIP SIETINIO TINKLŲ SIETUVO DUOMENŲ TVARKYTOJOS ATSAKOMYBĖ UŽ TARPVALSTYBINĮ NACIONALINIŲ KONTAKTŲ ATSEKIMO IR ĮSPĖJIMO PROGRAMĖLIŲ VIENŲ KITOMS PERDUODAMŲ DUOMENŲ TVARKYMĄ

Komisija:

1) sukuria ir užtikrina saugią ir patikimą ryšių infrastruktūrą, kuri sujungia sietinio tinklų sietuvo sistemoje dalyvaujančių valstybių narių nacionalines kontaktų atsekimo ir įspėjimo programėles. Kad įvykdytų savo sietinio tinklų sietuvo duomenų tvarkytojos įsipareigojimus, Komisija gali kaip pagalbines duomenų tvarkytojas įtraukti trečiąsias šalis; Komisija informuoja bendrus duomenų valdytojus apie bet kokius numatomus pakeitimus, susijusius su kitų pagalbinių duomenų tvarkytojų įtraukimu arba pakeitimu, taip suteikdama duomenų valdytojams galimybę pateikti bendrą prieštaravimą dėl tokių pakeitimų, kaip išdėstyta II priedo 1 skirsnio 1 poskirsnio 4 punkte. Komisija užtikrina, kad minėtiems papildomiems duomenų tvarkytojams būtų taikomi tokie patys duomenų apsaugos įpareigojimai, kokie nustatyti šiame sprendime;

2) tvarko asmens duomenis tik pagal duomenų valdytojų dokumentais įformintus nurodymus, išskyrus atvejus, kai tai daryti reikalaujama pagal Sąjungos arba valstybės narės teisę. Tokiu atveju Komisija prieš pradėdama tvarkyti duomenis praneša apie tokį teisinį reikalavimą duomenų valdytojams, išskyrus atvejus, kai pagal tą teisę toks pranešimas yra draudžiamas dėl svarbių viešojo intereso priežasčių;

3) tvarkydama duomenis Komisija:

a) nustato nacionalinių vidinių serverių tapatumą remdamasi nacionalinių vidinių serverių sertifikatais;

b) gauna Įgyvendinimo sprendimo 7a straipsnio 3 dalyje nurodytus duomenis, kuriuos įkelia nacionaliniai vidiniai serveriai, suteikdama programų sąsają, suteikiančią galimybę nacionaliniams vidiniams serveriams įkelti atitinkamus duomenis;

c) gavusi duomenis iš nacionalinių vidinių serverių, saugo juos sietiniame tinklų sietuve;

d) suteikia galimybę nacionaliniams vidiniams serveriams parsisiųsti duomenis;

e) ištrina duomenis po to, kai juos parsisiunčia visi dalyvaujantys vidiniai serveriai, arba praėjus 14 dienų nuo jų gavimo, atsižvelgiant į tai, kuri data ankstesnė;

f) baigus teikti paslaugą – ištrina visus likusius duomenis, išskyrus atvejus, kai asmens duomenis reikalaujama saugoti pagal Sąjungos arba valstybės narės teisę.

Duomenų tvarkytojas imasi visų būtinų priemonių tvarkomų duomenų vientisumui išsaugoti;

4) imasi visų pažangiausių organizacinių, fizinių ir loginių saugumo priemonių sietiniam tinklų sietuvui prižiūrėti. Šiuo tikslu Komisija:

a) paskiria subjektą, atsakingą už saugumo valdymą sietinio tinklų sietuvo lygmeniu, perduoda duomenų valdytojams jo kontaktinius duomenis ir užtikrina jo prieinamumą tuo atveju, kai reikia reaguoti į grėsmes saugumui;

b) prisiima atsakomybę už sietinio tinklų sietuvo saugumą;

c) užtikrina, kad visiems asmenims, kuriems suteikta prieiga prie sietinio tinklų sietuvo, būtų taikomi sutartiniai, profesiniai arba teisės aktais nustatyti konfidencialumo įpareigojimai;

5) imasi visų būtinų saugumo priemonių, kad išvengtų sklandaus nacionalinių vidinių serverių veikimo sutrikdymo. Šiuo tikslu Komisija įdiegia specialias procedūras, susijusias su vidinių serverių ir sietinio tinklų sietuvo ryšiu. Jos apima:

a) rizikos vertinimo siekiant nustatyti ir įvertinti galimas grėsmes sistemai procedūrą;

b) audito ir peržiūros procedūrą siekiant:

i. tikrinti įgyvendintų saugumo priemonių ir taikomos saugumo politikos atitiktį;

ii. reguliariai tikrinti sistemos rinkmenų vientisumą, saugumo parametrus ir suteiktus leidimus;

iii. stebėti, kad būtų galima aptikti saugumo pažeidimus ir įsilaužimus;

iv. atlikti pakeitimus siekiant sumažinti esamus saugumo trūkumus;

v. suteikti galimybę, taip pat duomenų valdytojų prašymu, atlikti nepriklausomus auditus, įskaitant tikrinimus, ir saugumo priemonių peržiūras ir prisidėti prie jų, jei tenkinamos sąlygos, kuriomis laikomasi SESV Protokolo (Nr. 7) dėl Europos Sąjungos privilegijų ir imunitetų ([2]);

([2]) Protokolas (Nr. 7) dėl Europos Sąjungos privilegijų ir imunitetų (OL C 326, 2012 10 26, p. 266).

c) kontrolės procedūros pakeitimą siekiant dokumentuoti ir įvertinti pakeitimo poveikį iki jo įgyvendinimo ir informuoti duomenų valdytojus apie visus pakeitimus, kurie gali paveikti ryšį su jų infrastruktūra ir (arba) jų infrastruktūros saugumą;

d) techninės priežiūros ir remonto tvarkos nustatymą siekiant nurodyti taisykles ir sąlygas, kurių turi būti laikomasi atliekant įrangos techninę priežiūrą ir (arba) remontą;

e) saugumo incidentų tvarkymo procedūros nustatymą siekiant apibrėžti pranešimų ir perdavimo spręsti aukštesniu lygmeniu sistemą, kad būtų galima nedelsiant informuoti duomenų valdytojus ir Europos duomenų apsaugos priežiūros pareigūną apie bet kokį asmens duomenų saugumo pažeidimą ir nustatyti drausmines procedūras saugumo pažeidimų atvejais;

6) imasi pažangiausių fizinio ir (arba) loginio saugumo priemonių, skirtų naudoti patalpose, kuriose yra sietinio tinklų sietuvo įranga, ir prieigos prie loginių duomenų bei saugios prieigos kontrolei. Šiuo tikslu Komisija:

a) užtikrina, kad būtų taikomos fizinio saugumo priemonės, kad būtų nustatyta aiški apsaugos zona ir aptinkami pažeidimai;

b) kontroliuoja prieigą prie patalpų ir registruoja lankytojus atsekamumo tikslais;

c) užtikrina, kad išorės asmenys, kuriems suteikta teisė patekti į patalpas, būtų lydimi tinkamai įgaliotų darbuotojų;

d) užtikrina, kad įrangos nebūtų galima papildyti, pakeisti arba pašalinti be išankstinio paskirtųjų atsakingų įstaigų leidimo;

e) kontroliuoja prieigą iš nacionalinių vidinių serverių prie sietinio tinklų sietuvo ir atvirkščiai;

f) užtikrina, kad asmenys, prisijungiantys prie sietinio tinklų sietuvo, būtų identifikuojami ir būtų patvirtinama jų tapatybė;

g) peržiūri leidimo teises, susijusias su prieiga prie sietinio tinklų sietuvo, jeigu padaromas šią infrastruktūrą veikiantis saugumo pažeidimas;

h) palaiko informacijos, perduodamos per sietinį tinklų sietuvą, vientisumą;

i) įgyvendina technines ir organizacines saugumo priemones, kad užkirstų kelią neteisėtai prieigai prie asmens duomenų;

j) prireikus įgyvendina priemones, skirtas neteisėtai prieigai prie sietinio tinklų sietuvo iš nacionalinių institucijų domeno blokuoti (t. y. blokuoja vietą arba IP adresą);

7) imasi veiksmų, kad apsaugotų savo domeną, įskaitant ryšių nutraukimą, jeigu nustatomas esminis nukrypimas nuo kokybės arba saugumo principų ir koncepcijų;

8) taiko su jos atsakomybės sritimi susijusį rizikos valdymo planą;

9) realiuoju laiku stebi visų jos teikiamų sietinio tinklų sietuvo paslaugų komponentų veikimą, reguliariai rengia statistinius duomenis ir saugo įrašus;

10) teikia su visomis sietinio tinklų sietuvo paslaugomis susijusią paramą anglų kalba 24 valandas per parą ir 7 dienas per savaitę telefonu, paštu arba per interneto portalą ir priima leidimą skambinti turinčių asmenų – sietinio tinklų sietuvo koordinatorių ir atitinkamų jų pagalbos tarnybų, projektų pareigūnų ir Komisijos paskirtų asmenų – skambučius;

11) padeda duomenų valdytojams taikydama tinkamas technines ir organizacines priemones, kiek tai įmanoma, kad būtų įvykdytas duomenų valdytojo įpareigojimas atsakyti į prašymus pasinaudoti Bendrojo duomenų apsaugos reglamento III skyriuje nustatytomis duomenų subjekto teisėmis;

12) padeda duomenų valdytojams teikdama informaciją apie sietinį tinklų sietuvą, kad būtų įgyvendinti Bendrojo duomenų apsaugos reglamento 32, 35 ir 36 straipsniuose nustatyti įpareigojimai;

13) užtikrina, kad sietiniame tinklų sietuve tvarkomi duomenys asmeniui, neturinčiam prieigos prie jo leidimo, būtų nesuprantami;

14) imasi visų tinkamų priemonių, kad užkirstų kelią sietinio tinklų sietuvo operatorių neteisėtai prieigai prie perduodamų duomenų;

15) imasi priemonių, kad palengvintų sietinio tinklų sietuvo paskirtųjų duomenų valdytojų tarpusavio sąveiką ir komunikaciją;

16) pagal Reglamento (ES) 2018/1725 31 straipsnio 2 dalį tvarko su duomenų tvarkymo veikla, vykdoma duomenų valdytojų vardu, susijusius įrašus.“